MANAJEMEN RISIKO KECURANGAN PADA UMKM DIGITAL: TINJAUAN SISTEMATIS KEAMANAN SIBER, PENGENDALIAN, DAN TEKNOLOGI ANTIFRAUD

Amanda[1]*, Billah Izza Muthmainnah[2], Nasha Rabilah Affandy[3], Novita[4]

[1, 2, 3, 4]Program Studi Akuntansi, Fakultas Ekonomi, Bisnis, dan Humaniora, Universitas Trilogi, Jakarta Selatan, Indonesia

amanda@trilogi.ac.id[1*],billahizzam@trilogi.ac.id[2],nasharabilah3009@trilogi.ac.id[3], novita_1210@trilogi.ac.id[4]

ABSTRAK

Penelitian ini mengkaji secara sistematis *fraud risk management* pada usaha mikro, kecil, dan menengah (UMKM) yang sedang mengalami transformasi digital dengan mengintegrasikan bukti empiris mengenai *cybersecurity*, *internal control*, *forensic accounting*, dan *anti-fraud technology*. Kajian dilakukan melalui *systematic literature review* terhadap publikasi terindeks Scopus yang didukung oleh referensi metodologis. Artikel yang terpilih dianalisis menggunakan *thematic synthesis* berdasarkan empat tema utama, yaitu *internal fraud* dan faktor perilaku, ancaman *cybersecurity* dan risiko akuntansi digital, *anti-fraud technology* dan *data analytics*, serta *governance*, kepatuhan, *forensic accounting*, dan ketahanan terhadap *fraud*. Hasil kajian menunjukkan bahwa risiko *fraud* pada UMKM digital bersifat *socio-technical* karena dipengaruhi oleh interaksi antara faktor perilaku, sistem pengendalian, dan teknologi. Berbagai teknologi, seperti *data analytics*, *machine learning*, AI-enabled *mobile money*, *smart contracts*, dan *user-behavior analytics*, terbukti berpotensi meningkatkan efektivitas pencegahan *fraud*. Namun, implementasinya dipengaruhi oleh kualitas *governance*, *explainability*, kualitas data, keterjangkauan biaya, dan kesiapan organisasi. Kajian ini mengintegrasikan perspektif teori *fraud*, *cybersecurity assurance*, *internal control*, *forensic accounting*, dan ketahanan digital melalui suatu *socio-technical framework* yang menempatkan *fraud risk management* sebagai kapabilitas adaptif dalam menghadapi risiko *fraud* pada era transformasi digital.

Kata kunci: *Anti-fraud technology*; *Cybersecurity assurance*; *Digital resilience*; *Fraud risk management*; Usaha Mikro, Kecil, dan Menengah (UMKM)

ABSTRACT

This study systematically reviews fraud risk management in small and medium-sized enterprises (SMEs) undergoing digital transformation by integrating empirical evidence on cybersecurity, internal control, forensic accounting, and anti-fraud technology. The review was conducted using a systematic literature review of Scopus-indexed publications supported by methodological references. The selected studies were analyzed through thematic synthesis based on four major themes: internal fraud and behavioral drivers, cybersecurity threats and digital accounting risks, anti-fraud technology and data analytics, and governance, compliance, forensic accounting, and fraud resilience. The findings indicate that fraud risk in digital SMEs is socio-technical in nature, resulting from the interaction of behavioral factors, control systems, and digital technologies. Technologies such as data analytics, machine learning, AI-enabled mobile money, smart contracts, and user-behavior analytics demonstrate significant potential to strengthen fraud prevention. However, their effectiveness depends on the quality of governance, explainability, data quality, affordability, and organizational readiness. This review integrates perspectives from fraud theory, cybersecurity assurance, internal control, forensic accounting, and digital resilience into a socio-technical framework

that positions fraud risk management as an adaptive organizational capability for addressing fraud risks in the digital transformation era.

Keywords: *Anti-fraud technology*; *Cybersecurity assurance*; *Digital resilience*; *Fraud risk management*; Small and Medium-sized Enterprises (SMEs)
*billahizzam@trilogi.ac.id ✉

PENDAHULUAN

Usaha kecil dan menengah (UKM) memiliki posisi strategis dalam penciptaan lapangan kerja, pengembangan entrepreneurship, penguatan regional resilience, dan pembangunan ekonomi yang inklusif. Peran tersebut semakin menonjol di negara berkembang dan emerging economies karena UKM menyediakan peluang kerja yang relatif mudah diakses, mendorong keterlibatan dalam *local supply chain*, serta membuka jalur bagi pelaku usaha untuk memasuki pasar formal. Meskipun demikian, UKM memiliki kerentanan struktural terhadap *fraud* karena umumnya beroperasi dengan cadangan keuangan yang terbatas, kewenangan manajerial yang terkonsentrasi, *segregation of duties* yang lemah, sistem pelaporan informal, serta keterbatasan akses terhadap tenaga ahli dalam bidang accounting, auditing, legal, dan *cybersecurity*. Kondisi tersebut sejalan dengan temuan bahwa keterbatasan sumber daya, lemahnya keahlian, dan rendahnya formalitas sistem menjadi penghambat penerapan *risk management* yang efektif pada UKM (Brustbauer, 2016; Chakabva et al., 2021; Ferreira de Araújo Lima et al., 2020). Keterbatasan akses terhadap dukungan *accounting* dan pengelolaan risiko juga dapat mengurangi kemampuan UKM dalam membangun prosedur pengawasan dan pengendalian yang memadai (Moschella et al., 2023). Oleh karena itu, berbagai bentuk *traditional fraud*, seperti *stealing*, *fake currency*, *non-payment*, *embezzlement*, dan *accounting fraud*, tetap menjadi risiko yang memberikan konsekuensi serius. Pada UKM di Ghana, Andoh et al. (2018) menemukan bahwa *stealing, fake currency*, serta *non-payment* atas barang atau jasa mencakup hampir 83% dari seluruh kasus *fraud* yang dilaporkan. Penelitian tersebut juga menunjukkan bahwa *accounting fraud* merupakan satu-satunya variabel *fraud* yang memiliki pengaruh negatif dan signifikan secara statistik terhadap pertumbuhan UKM. Bukti tersebut menegaskan bahwa fraud bukan sekadar persoalan operasional yang bersifat marginal, melainkan kendala langsung terhadap keberlangsungan dan perkembangan UKM.

Digital transformation telah memperbesar kompleksitas permasalahan *fraud* dengan memperluas peluang sekaligus tingkat paparan risiko yang dihadapi UKM (Hanelt et al., 2021; Kraus et al., 2021; Verhoef et al., 2021). Dalam menjalankan kegiatan usahanya, UKM semakin bergantung pada *e-commerce platforms*, *digital payment systems*, *mobile money*, *online marketplaces*, *cloud accounting*, *web applications*, dan *AI-enabled business processes*. Pemanfaatan digital technologies tersebut dapat meningkatkan efisiensi, memperluas jangkauan pelanggan, memperkuat *logistics knowledge*, mendorong *financial inclusion*, serta mempercepat proses transaksi. Mohamad et al. (2026), misalnya, menemukan bahwa *AI-powered mobile money systems* mampu meningkatkan kepercayaan, memperkuat *logistics knowledge*, dan membantu UKM dalam rantai pasok di Nigeria mengatasi hambatan transaksi yang berkaitan dengan *fraud*. Namun, *digitalization* juga menciptakan attack surfaces baru yang dapat dimanfaatkan oleh pelaku *fraud*. UKM menghadapi berbagai ancaman, seperti *phishing*, *ransomware*, *business email compromise*, *invoice fraud*, *unauthorized access*, *credit-card fraud*, *payment-gateway manipulation*, *search-engine poisoning*, *deceptive platform credibility cues*, dan *vulnerabilities in web applications* (Aslan et al., 2023; Le et al., 2024; Khan et al., 2025; Loskorikh et al., 2025). Low (2017) melaporkan bahwa berdasarkan survei Pemerintah Inggris, rata-rata biaya yang ditimbulkan oleh *cybersecurity breach* pada UKM berkisar antara £75.000 hingga £311.000. Temuan tersebut menunjukkan besarnya konsekuensi finansial dari *cyber-enabled fraud* bagi perusahaan yang memiliki keterbatasan sumber daya.

Dalam kajian ini, digital SMEs didefinisikan sebagai *small and medium-sized enterprises* yang mengadopsi atau bergantung pada *digital technologies*, termasuk *e-commerce*

platforms, *digital payment systems*, *mobile applications*, *cloud accounting*, *web applications*, *digital supply-chain systems*, dan *online customer interfaces* (Bharadwaj et al., 2013; Nambisan, 2017; Vial, 2019; Verhoef et al., 2021). *Fraud risk management* dimaknai sebagai proses sistematis yang meliputi identifikasi, pencegahan, pendeteksian, respons, dan pemantauan terhadap *fraud-related threats* yang mempengaruhi aset, transaksi, data, serta kepercayaan (Albrecht et al., 2019; Jans et al., 2009). *Cybersecurity* mengacu pada perlindungan terhadap *digital systems*, *networks*, *applications*, dan data dari *unauthorized access*, *disruption*, *misuse*, dan *attack* (Aslan et al., 2023; Bozkus Kahyaoglu & Caliyurt, 2018). *Internal control* merujuk pada *policies*, *procedures*, *authorization mechanisms*, *monitoring routines*, dan *accountability structures* yang dirancang untuk mencegah serta mendeteksi *error*, *fraud*, dan *misuse* (Jans et al., 2009; Moschella et al., 2023). Sementara itu, *anti-fraud technology* didefinisikan sebagai berbagai digital tools yang digunakan untuk mencegah, mendeteksi, memantau, atau merespons *fraud*, termasuk *data analytics*, AI, *machine learning*, *anomaly detection*, *multi-factor authentication*, *transaction monitoring*, *blockchain*, *smart contracts*, dan *user-behavior analytics* (Ngai et al., 2011; Carcillo et al., 2021; Ridha Tarigan et al., 2025; Rugeles Diaz et al., 2025; Zirar et al., 2026).

Kajian ini didasarkan pada lima research questions. Pertama, jenis *fraud risks* apa yang paling sering dibahas dalam literatur mengenai SMEs yang sedang mengalami digital transformation? Kedua, bagaimana *cybersecurity*, *internal control*, dan *forensic accounting* berkontribusi terhadap *fraud risk management* pada digital SMEs? Ketiga, jenis anti-fraud technologies apa yang digunakan untuk mencegah, mendeteksi, atau mengurangi fraud dalam SME digital environments? Keempat, perspektif teoritis apa yang dapat menjelaskan *fraud risk* dan *fraud resilience* pada *digital SMEs*? Kelima, *research gaps* apa yang masih terdapat dalam pengembangan *fraud risk management frameworks* bagi *SMEs* yang bersifat *scalable*, *affordable*, dan *context-sensitive*?

Riset ini memberikan tiga kontribusi terhadap literatur. Pertama, penelitian ini mengintegrasikan berbagai bukti yang mencakup i*nternal fraud, cyber fraud, accounting control, cybersecurity assurance, payment fraud, AI-enabled detection, blockchain, smart contracts,* dan *digital resilience* (Bozkus Kahyaoglu & Caliyurt, 2018; Ngai et al., 2011; Rugeles Diaz et al., 2025; Zirar et al., 2026). Kedua, penelitian ini mengembangkan interpretasi *socio-technical* mengenai *SME fraud risk* dengan menegaskan bahwa *fraud* muncul melalui interaksi antara *human behavior, opportunity structures, digital vulnerabilities, weak governance,* dan *resource constraints* (Cressey, 1950; Chakabva et al., 2021; Ridha Tarigan et al., 2025; Wolfe & Hermanson, 2004). Ketiga, penelitian ini menempatkan *fraud risk management* sebagai *adaptive capability*, yang mengharuskan *SMEs* untuk mengidentifikasi ancaman yang sedang berkembang, menerapkan kontrol dan teknologi yang sesuai, serta menyesuaikan kembali rutinitas ketika teknik fraud terus mengalami perubahan (Eisenhardt & Martin, 2000; Teece et al., 1997; Teece, 2007). Kerangka tersebut menghubungkan *fraud triangle theory* dan *fraud diamond theory* dengan *resource-based view, dynamic capabilities, forensic accounting,* dan *cybersecurity assurance* (Barney, 1991, 2001; Cressey, 1950; Kumari Tiwari & Debnath, 2017; Wolfe & Hermanson, 2004).

PENGEMBANGAN KERANGKA TEORITIS

Teori Fraud dan Landasan Perilaku Risiko Fraud pada UMKM

Teori *Fraud Triangle Theory* menjelaskan bahwa perilaku *fraud* terjadi sebagai hasil interaksi antara tiga elemen utama, yaitu tekanan (*pressure*), peluang (*opportunity*), dan rasionalisasi (*rationalization*) (Cressey, 1950). Dalam konteks usaha mikro, kecil, dan menengah (UMKM), tekanan dapat bersumber dari berbagai kondisi, seperti kesulitan arus kas, kebutuhan finansial pribadi, ketidakpastian pekerjaan, maupun tuntutan untuk mencapai target kinerja. Di sisi lain, peluang terjadinya *fraud* dapat muncul akibat lemahnya pemisahan tugas, prosedur persetujuan yang masih bersifat informal, tingginya ketergantungan terhadap pemilik atau manajer, terbatasnya aktivitas pengawasan, serta dokumentasi transaksi yang kurang memadai. Sementara itu, rasionalisasi memungkinkan individu membenarkan tindakan yang tidak etis dengan menganggap bahwa perilaku tersebut hanya bersifat sementara, merupakan sesuatu yang pantas diterima, tidak menimbulkan dampak yang berarti, atau bahkan dianggap sebagai suatu kebutuhan.

Selanjutnya, *Fraud Diamond Theory* mengembangkan konsep tersebut dengan menambahkan unsur kapabilitas (*capability*) sebagai faktor keempat. Menurut teori ini, keberadaan tekanan, peluang, dan rasionalisasi saja belum cukup untuk mendorong terjadinya *fraud* apabila pelaku tidak memiliki kemampuan untuk memanfaatkan peluang yang tersedia (Wolfe & Hermanson, 2004). Dalam lingkungan UMKM yang telah terdigitalisasi, aspek kapabilitas menjadi semakin penting karena karyawan, vendor, pengguna platform digital, maupun pihak eksternal berpotensi menyalahgunakan hak akses, memanfaatkan kelemahan kata sandi, sistem berbasis *cloud*, perangkat lunak akuntansi, antarmuka pembayaran digital, maupun celah keamanan pada aplikasi berbasis web.

Berbagai penelitian empiris menunjukkan bahwa teori-teori perilaku tersebut masih sangat relevan dalam menjelaskan terjadinya *fraud* pada era digital. Ridha Tarigan et al. (2025) menemukan bahwa rasionalisasi memiliki pengaruh yang signifikan terhadap perilaku *fraud* karyawan pada UMKM kedai kopi di Indonesia. Penelitian tersebut juga menunjukkan bahwa penerapan teknologi *anti-fraud* mampu memoderasi hubungan antara peluang, rasionalisasi, dan perilaku *fraud*. Hasil tersebut sejalan dengan penelitian Andoh et al. (2018) yang mengemukakan bahwa *fraud* internal pada UMKM merupakan konsekuensi dari interaksi antara lemahnya sistem pengendalian, perilaku karyawan, serta kelemahan dalam sistem akuntansi. Di sisi lain, *fraud* pada platform digital menghadirkan dimensi perilaku yang lebih kompleks. Oo et al. (2025) menunjukkan bahwa kampanye *crowdfunding* yang bersifat *fraud* dapat memanfaatkan persepsi subjektif pengguna melalui indikator seperti tingkat kepercayaan (*trustworthiness*) dan daya tarik (*attractiveness*). Dengan demikian, *fraud* pada UMKM berbasis digital tidak hanya berkaitan dengan eksploitasi terhadap aspek teknis sistem, tetapi juga dipengaruhi oleh persepsi legitimasi, iklim etika organisasi, serta manipulasi perilaku yang dilakukan oleh para pelaku.

Keamanan Siber, Pengendalian Internal, dan Akuntansi Forensik sebagai Pengendalian Sosio-Teknis

Cybersecurity, *internal control*, dan *forensic accounting* merupakan tiga komponen yang saling melengkapi dalam upaya pengelolaan risiko *fraud*. *Cybersecurity* berfungsi melindungi infrastruktur digital, jaringan, aplikasi, identitas pengguna, serta data dari berbagai ancaman keamanan. Sementara itu, *internal control* berperan dalam mengatur mekanisme otorisasi, verifikasi transaksi, pemisahan tugas, pengelolaan hak akses, aktivitas pemantauan, *audit trail*, dan akuntabilitas organisasi. Di sisi lain, *forensic accounting*

memberikan pendekatan investigatif melalui interpretasi bukti, penilaian risiko *fraud*, serta integrasi keahlian di bidang akuntansi, audit, hukum, dan analisis (Kumari Tiwari & Debnath, 2017). Dalam lingkungan digital, ruang lingkup *forensic accounting* juga mencakup penanganan bukti digital, manipulasi yang difasilitasi oleh teknologi, serta berbagai bentuk *fraud* berbasis teknologi (Daraojimba et al., 2023). Selaras dengan hal tersebut, Bozkus Kahyaoglu dan Caliyurt (2018) berpendapat bahwa *cybersecurity assurance* perlu dipandang sebagai bagian dari fungsi audit internal karena memiliki keterkaitan yang erat dengan risiko siber, integritas data, dan tata kelola teknologi.

Ketiga mekanisme pengendalian tersebut bersifat *socio-technical* karena efektivitasnya bergantung pada keterpaduan antara sumber daya manusia, proses bisnis, dan teknologi. Loskorikh et al. (2025) menunjukkan bahwa penerapan *multi-factor authentication*, pelatihan bagi karyawan, serta kolaborasi yang terintegrasi antara fungsi teknologi informasi dan akuntansi mampu menurunkan kemungkinan terjadinya serangan siber sekaligus meningkatkan efektivitas respons terhadap insiden pada lingkungan akuntansi. Selain itu, Moschella et al. (2023) menjelaskan bahwa akuntan memiliki kontribusi penting dalam pengelolaan risiko UMKM melalui penerapan disiplin pelaporan, pemberian rekomendasi terkait pengendalian, serta dukungan dalam pengambilan keputusan. Temuan tersebut mengindikasikan bahwa batas antara pengendalian akuntansi dan pengendalian *cybersecurity* semakin tidak terpisahkan pada UMKM berbasis digital. Sebagai contoh, suatu kasus *payment fraud* dapat terjadi akibat kombinasi beberapa kelemahan secara bersamaan, seperti prosedur otorisasi yang kurang memadai, kredensial pengguna yang telah dikompromikan, lemahnya proses peninjauan akuntansi, minimnya pelatihan bagi karyawan, serta kurang optimalnya pemantauan terhadap transaksi.

Teknologi *Anti-Fraud*, *Dynamic Capabilities*, dan Ketahanan Digital UMKM

Teknologi *anti-fraud* mencakup berbagai solusi digital, seperti *data analytics*, *artificial intelligence (AI)*, *machine learning*, *anomaly detection*, *user-behavior analytics*, *multi-factor authentication*, *transaction monitoring*, *blockchain*, *smart contracts*, serta *secure software testing*. Kontribusi teoretis dari teknologi tersebut dapat dijelaskan melalui perspektif *resource-based view* dan *dynamic capabilities*. Menurut *resource-based view*, sumber daya yang bernilai, langka, sulit ditiru, dan terintegrasi dalam organisasi mampu menciptakan serta mempertahankan keunggulan kompetitif (Barney, 1991, 2001). Dalam konteks UMKM berbasis digital, budaya organisasi yang memiliki kesadaran terhadap keamanan siber, pengetahuan mengenai *forensic accounting*, prosedur *internal control*, dan kemampuan analisis *fraud* dapat dipandang sebagai sumber daya strategis. Sementara itu, teori *dynamic capabilities* menjelaskan kemampuan organisasi dalam mengenali ancaman, memanfaatkan peluang untuk merespons perubahan, serta melakukan rekonfigurasi kompetensi sesuai dengan dinamika lingkungan bisnis (Eisenhardt & Martin, 2000; Teece et al., 1997; Teece, 2007). Perspektif ini sangat relevan dalam pengelolaan risiko *fraud* mengingat pelaku *fraud* terus mengembangkan modus operandi, teknologi mengalami perkembangan yang cepat, dan UMKM dituntut untuk memperbarui mekanisme pengendaliannya secara berkelanjutan.

Awolowo et al. (2026) secara eksplisit mengintegrasikan budaya organisasi, *fraud risk management*, *forensic accounting*, *resource-based view*, dan *dynamic capabilities* dalam menjelaskan *cybersecurity assurance* pada UMKM. Sementara itu, Rugeles Diaz et al. (2025) menunjukkan bahwa kinerja model *machine learning* dalam mendeteksi *fraud* berbeda-beda bergantung pada ukuran pedagang (*merchant*) serta karakteristik transaksi yang dianalisis. Temuan tersebut mengindikasikan bahwa penerapan teknologi perlu disesuaikan dengan

kapasitas dan model bisnis masing-masing UMKM. Selain itu, Zirar et al. (2026) mengemukakan bahwa *smart contracts* mampu meningkatkan transparansi, keterlacakan (*traceability*), dan kepercayaan (*trust*) dalam transaksi UMKM. Meskipun demikian, implementasi teknologi tersebut memerlukan penyesuaian model bisnis serta kesiapan tata kelola organisasi. Secara keseluruhan, berbagai teori tersebut mendukung perspektif ketahanan (*resilience*) yang menegaskan bahwa UMKM berbasis digital tidak hanya membutuhkan teknologi sebagai alat pendukung, tetapi juga memerlukan budaya belajar, budaya etika, komitmen manajerial, struktur tata kelola yang memadai, serta kemampuan adaptif agar mampu menghadapi risiko *fraud* secara berkelanjutan.

METODE, DATA, DAN ANALISIS

Kajian ini menggunakan desain *systematic literature review* karena bertujuan untuk mengidentifikasi, mengorganisasi, dan mensintesis bukti empiris, konseptual, serta metodologis mengenai *fraud risk management* pada *SMEs* yang sedang mengalami digital transformation. Kerangka metodologis penelitian mengacu pada prinsip transparansi dalam PRISMA 2020 yang menekankan pentingnya pelaporan secara jelas mengenai alasan pelaksanaan kajian, prosedur yang digunakan, dan bukti yang diperoleh (Page et al., 2021). Selain itu, kajian ini mengikuti pedoman *systematic review* dalam bidang manajemen dan ilmu sosial, khususnya yang berkaitan dengan kejelasan *search logic, eligibility criteria, data extraction,* dan *thematic synthesis* (Grant & Booth, 2009; Higgins et al., 2024; Tranfield et al., 2003; Xiao & Watson, 2019). Karena dasar bukti yang digunakan bersifat heterogen dan mencakup bidang *accounting, cybersecurity, information systems, fraud analytics,* serta *SME risk management,* maka *thematic synthesis* dinilai lebih sesuai dibandingkan *meta-analysis.*

Strategi Pencarian

Search logic disusun dengan menggabungkan tiga blok konsep, yaitu istilah yang berkaitan dengan *fraud* dan *fraud risk, digital technology,* serta *SME*, sebagaimana pendekatan pencarian sistematis yang menekankan penggunaan kombinasi konsep dan kata kunci secara eksplisit (Okoli & Schabram, 2010; Tranfield et al., 2003; Xiao & Watson, 2019). Istilah *fraud* mencakup *fraud risk, fraud prevention, fraud detection, internal fraud, accounting fraud, cyber fraud, digital fraud, financial fraud, payment fraud, credit-card fraud, invoice fraud, unethical behavior,* dan *corruption.* Istilah *technology* meliputi *digital transformation, digitalization, digital payment, mobile money, fintech, cloud accounting, web application, cybersecurity, cyber resilience, artificial intelligence, machine learning, data analytics, blockchain,* dan *smart contract.* Sementara itu, istilah *SME* terdiri atas *SME, SMEs, small and medium enterprises, small and medium-sized enterprises, small business, medium-sized business, MSME,* dan *digital SME.* Strategi pencarian tersebut dirancang untuk menjangkau studi yang secara khusus membahas SME serta penelitian lain yang temuan dan pembahasannya dapat diterapkan pada *digital fraud* dan *fraud risk management.*

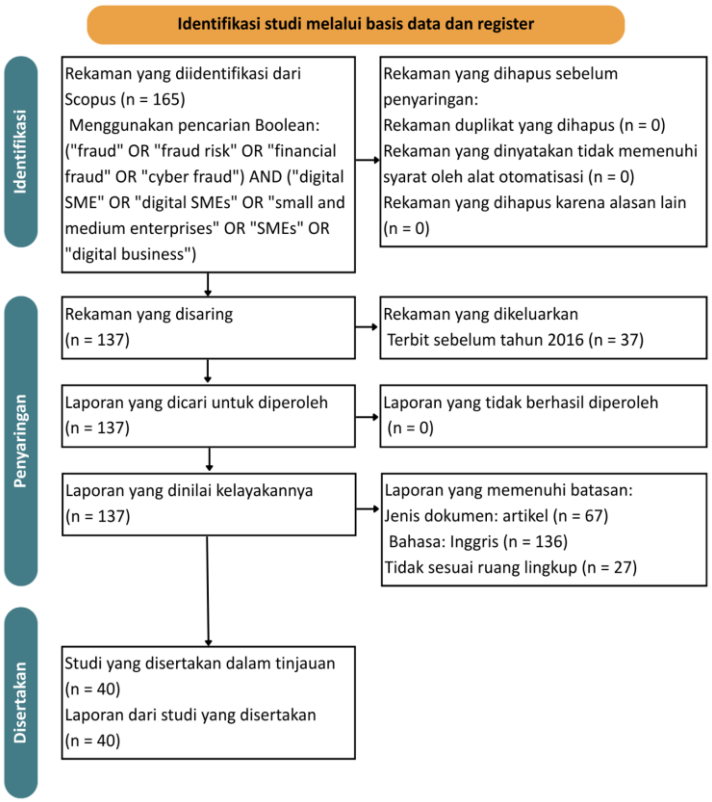
Kriteria Kelayakan

Studi dimasukkan ke dalam kajian apabila membahas sekurang-kurangnya satu domain berikut: *SME fraud risk, digital fraud, cyber fraud, internal fraud, accounting fraud, payment fraud, digital accounting risk, cybersecurity in SMEs, internal control, forensic accounting, anti-fraud technology, AI or machine-learning fraud detection, blockchain or smart contracts for transaction assurance,* atau *digital resilience.* Penetapan kriteria tersebut dilakukan untuk memastikan bahwa setiap literatur yang dipilih memiliki keterkaitan langsung dengan fokus dan pertanyaan kajian (Tranfield et al., 2003; Xiao & Watson, 2019). Literatur yang memenuhi

kriteria mencakup artikel jurnal yang telah melalui proses *peer review, review articles*, serta makalah konferensi atau konseptual berkualitas tinggi yang memberikan kontribusi jelas terhadap pertanyaan kajian. Sebaliknya, studi dikeluarkan apabila hanya berfokus pada perusahaan besar, bank, atau institusi publik tanpa memiliki relevansi yang dapat diterapkan pada SMEs. Studi juga tidak disertakan apabila hanya membahas *generic cybersecurity* tanpa keterkaitan dengan *fraud, risk, control, atau SMEs*, serta apabila informasi bibliografis dan metodologisnya tidak memadai untuk mendukung proses pengkodean yang dapat diandalkan (Page et al., 2021; Tranfield et al., 2003).

Penyaringan, Seleksi, dan Analisis Risiko Bias

Seluruh records disaring secara bertahap berdasarkan relevansi judul, abstrak, kata kunci, dan *full record* sesuai dengan prinsip transparansi dalam pelaksanaan *systematic literature review* (Page et al., 2021; Xiao & Watson, 2019). *Final analytic corpus* terdiri atas 43 referensi unik yang dikelompokkan ke dalam empat *evidence tables*. Setiap studi dikodekan berdasarkan referensi, konteks, *fraud type* atau *threat, theoretical lens, metode atau data, key findings,* serta implikasinya terhadap fraud risk management. *Quality appraisal* dilakukan dengan mempertimbangkan kejelasan tujuan penelitian, relevansi terhadap *SMEs* atau *digital business*, transparansi metode, kesesuaian sumber data, validitas analisis, kekuatan bukti, dan keterterapan temuan pada konteks *digital SMEs* (Grant & Booth, 2009; Higgins et al., 2024). *Heterogenitas analytic corpus* mengharuskan penggunaan proses penilaian yang fleksibel. *Quantitative studies* dinilai berdasarkan sampel, model, dan kejelasan analisis; *qualitative studies* dievaluasi berdasarkan koherensi desain dan kredibilitas interpretasi; *technical studies* ditelaah berdasarkan v*ulnerability type, detection method,* dan *relevansi praktis*; sedangkan *conceptual studies* dinilai berdasarkan kontribusi teoretis dan keterterapannya.



Gambar 1. Diagram alir PRISMA proses penyaringan dan pemilihan literatur

HASIL

Internal Fraud, Faktor Perilaku, dan Kerentanan UMKM

Tabel 1 menyajikan sintesis berbagai temuan penelitian mengenai *internal fraud*, faktor-faktor perilaku, serta kerentanan yang dihadapi UMKM. Hasil kajian menunjukkan bahwa *internal fraud* konvensional masih menjadi permasalahan utama dalam lanskap risiko *fraud* pada UMKM yang telah terdigitalisasi. Andoh et al. (2018) memberikan bukti empiris dari UMKM di Ghana bahwa praktik pencurian, penggunaan uang palsu, dan kegagalan pembayaran menyumbang hampir 83% dari seluruh kasus *fraud*, sedangkan *accounting fraud* terbukti menghambat pertumbuhan UMKM secara signifikan. Temuan tersebut mengindikasikan bahwa proses digitalisasi tidak menghilangkan risiko *fraud* konvensional, tetapi justru menciptakan saluran baru yang dapat dimanfaatkan ketika sistem pengendalian masih lemah.

Penelitian Ridha Tarigan et al. (2025) memperkuat temuan tersebut dengan menunjukkan bahwa rasionalisasi berpengaruh signifikan terhadap perilaku *fraud*, sementara penerapan teknologi *anti-fraud* mampu memoderasi hubungan antara peluang (*opportunity*), rasionalisasi (*rationalization*), dan perilaku *fraud*. Dari perspektif teoretis, hasil tersebut semakin menegaskan relevansi *Fraud Triangle Theory* yang dikemukakan oleh Cressey (1950) serta *Fraud Diamond Theory* yang dikembangkan oleh Wolfe dan Hermanson (2004). Selain itu, temuan tersebut juga menunjukkan bahwa mekanisme pemantauan berbasis digital dapat memengaruhi persepsi individu terhadap peluang untuk melakukan *fraud*.

Berbagai bukti empiris yang berfokus pada aspek perilaku dan konteks organisasi semakin memperluas pemahaman mengenai fenomena tersebut. Kasa et al. (2023) menemukan adanya perbedaan kecenderungan melakukan kecurangan (*cheating propensity*) antar generasi dan sektor organisasi, termasuk pada UMKM. Hasil tersebut menunjukkan bahwa tingkat risiko *fraud* dipengaruhi oleh kondisi sosial maupun karakteristik organisasi. Sementara itu, Dellaportas (2013), Sham et al. (2023), Suh et al. (2019), serta Mintchik dan Riley (2019) secara kolektif menegaskan bahwa upaya pencegahan *fraud* perlu difokuskan pada pengurangan rasionalisasi, pembatasan peluang, serta penguatan sistem pengendalian di lingkungan kerja. Di sisi lain, Oo et al. (2025) memperkenalkan dimensi baru yang berkaitan dengan platform digital melalui temuannya bahwa kampanye *crowdfunding* yang bersifat *fraud* mampu memanfaatkan indikator kredibilitas subjektif pengguna. Oleh karena itu, strategi pencegahan *fraud* pada UMKM digital tidak hanya membutuhkan budaya etika yang kuat, tetapi juga akuntabilitas yang jelas, mekanisme verifikasi transaksi, jaminan identitas pengguna, serta sistem pengendalian yang mampu mengurangi peluang nyata maupun persepsi terhadap peluang untuk melakukan tindakan *fraud*.

Tabel 1. Ringkasan Temuan Utama mengenai *Internal Fraud*, Faktor Perilaku, dan Kerentanan UMKM

Referensi	Konteks	Metode/Data	Temuan Utama	Implikasi
Andoh et al. (2018)	UKM Ghana	Regresi potong lintang; 250 UKM	Kecurangan akuntansi menghambat pertumbuhan; pencurian, uang palsu, dan gagal bayar mencakup hampir 83% kasus.	Perkuat kontrol akuntansi, verifikasi pembayaran, dan pengamanan kas.
Ridha Tarigan et al. (2025)	UKM kedai kopi Indonesia	Survei 161 karyawan; analisis moderasi	Rasionalisasi berpengaruh; teknologi anti-kecurangan memoderasi kesempatan dan rasionalisasi.	Gunakan teknologi untuk memperkuat pemantauan.
Kasa et al. (2023)	UKM, perusahaan besar, sektor publik	Eksperimen korupsi berbasis agen	Kecenderungan berbuat curang berbeda menurut generasi & sektor.	Masukkan faktor perilaku dan konteks dalam penilaian risiko.
Oo et al. (2025)	Kampanye urun dana	204 kampanye; pasangan sepadan	Isyarat kredibilitas subjektif lebih kuat memprediksi keberhasilan kampanye curang.	Perkuat verifikasi dan tata kelola kredibilitas platform.
Cressey (1950)	Kecurangan pekerjaan	Teori dasar	Kecurangan muncul melalui tekanan, kesempatan, dan rasionalisasi.	Gabungkan etika, kesadaran tekanan, dan desain kontrol.
Wolfe & Hermanson (2004)	Kecurangan organisasi	Teori konseptual	Kecurangan memerlukan tekanan, kesempatan, rasionalisasi, dan kapabilitas.	Kurangi kesempatan dan kapabilitas pelaku.
Suh et al. (2019)	Kecurangan pekerjaan	Studi empiris risiko kecurangan	Pengurangan kesempatan & faktor risiko menekan	Terapkan pemisahan tugas dan penelaahan transaksi.

			terjadinya kecurangan.	
Dellaportas (2013)	Kasus kecurangan akuntansi	Wawancara kualitatif	Pelaku merasionalisasi pelanggaran ketika pengendalian lemah.	Lawan rasionalisasi melalui pelatihan dan akuntabilitas.
Sham et al. (2023)	Kecurangan di tempat kerja	Studi empiris segitiga kecurangan	Kecurangan karyawan terkait tekanan, kesempatan, dan rasionalisasi.	Tangani aspek perilaku dan sistem pengendalian.
Mintchik & Riley (2019)	Pencegahan kecurangan akuntansi	Analisis profesional/ akademik	Pemahaman rasionalisasi dapat memperkuat pencegahan.	Gunakan pelatihan skenario dan akuntabilitas yang terlihat.

Ancaman *Cybersecurity*, Risiko Akuntansi Digital, dan Kerentanan Aplikasi Web

Tabel 2 menyajikan ringkasan hasil penelitian mengenai hubungan antara risiko *fraud* pada UMKM digital dengan tingkat paparan terhadap ancaman *cybersecurity*. Low (2017) menunjukkan bahwa serangan siber dapat menimbulkan kerugian finansial yang signifikan bagi UMKM, dengan estimasi biaya pelanggaran keamanan (*data breach*) berkisar antara £75.000 hingga £311.000. Temuan ini diperkuat oleh Loskorikh et al. (2025) yang memberikan bukti empiris pada lingkungan akuntansi digital. Penelitian tersebut mengidentifikasi bahwa *phishing*, akses tanpa otorisasi (*unauthorized access*), dan *invoice fraud* merupakan ancaman utama yang dihadapi organisasi. Selain itu, penerapan *multi-factor authentication (MFA)* terbukti mampu menurunkan kemungkinan serangan siber sebesar 58%, pelatihan karyawan mengurangi tingkat risiko sebesar 37%, sedangkan kolaborasi antara tim teknologi informasi dan akuntansi yang terintegrasi mempercepat penyelesaian insiden hingga 40%. Hasil tersebut mendukung penerapan model pengendalian berlapis (*layered control model*), di mana mekanisme autentikasi, pelatihan, serta koordinasi lintas fungsi saling melengkapi dalam memperkuat pengendalian terhadap risiko *fraud*.

Selain ancaman terhadap sistem internal, kerentanan pada aplikasi web dan platform digital juga meningkatkan risiko *fraud*. Khan et al. (2025) menunjukkan bahwa berbagai kelemahan keamanan yang termasuk dalam *OWASP Top 10*, seperti *injection*, *broken authentication*, *sensitive data exposure*, dan *cross-site scripting (XSS)*, masih banyak ditemukan pada sistem bisnis digital. Di sisi lain, Le et al. (2024) mengidentifikasi *search-engine optimization (SEO) poisoning* sebagai ancaman eksternal yang dapat mengarahkan pengguna menuju situs berbahaya melalui manipulasi hasil pencarian. Sementara itu, Le et al. (2025) mengusulkan penerapan *user-behavior analytics* sebagai pendekatan untuk mengidentifikasi aktivitas pengguna yang bersifat tidak normal. Sejalan dengan temuan tersebut, Awan dan Alam (2025), Falch et al. (2023), serta Khan et al. (2025) menyimpulkan bahwa UMKM memerlukan dukungan *cybersecurity* yang bersifat skalabel, mudah diakses, dan disesuaikan dengan karakteristik organisasi, mengingat sebagian besar UMKM masih memiliki keterbatasan sumber daya dan keahlian internal. Oleh karena itu, *cybersecurity* seharusnya diposisikan sebagai bagian integral dari *fraud risk management*, bukan hanya sebagai fungsi teknis yang berdiri sendiri.

Tabel 2. Ringkasan Temuan Utama mengenai Ancaman *Cybersecurity*, Risiko Akuntansi Digital, dan Kerentanan Aplikasi Web

Referensi	Konteks	Metode/Data	Temuan Utama	Implikasi
Low (2017)	Pelanggaran siber UKM	Analisis industri	Biaya rata-rata pelanggaran UKM diperkirakan £75.000-£311.000.	Padukan asuransi siber, kesiapan, dan perencanaan kecurangan.
Loskorikh et al. (2025)	Sistem akuntansi digital	Wawancara, kasus, dan statistik	MFA menurunkan serangan 58%; pelatihan 37%; tim terpadu menangani insiden 40% lebih cepat.	Jadikan keamanan siber akuntansi bagian dari manajemen risiko kecurangan.
Khan et al. (2025a)	Aplikasi web	Pengujian OWASP dengan BeeWAP	Kerentanan utama: injeksi, autentikasi rusak, paparan data, dan XSS.	Lakukan pengujian kerentanan dan pengembangan aman.
Le et al. (2024)	Visibilitas digital UKM	Analisis ancaman	Peracunan SEO mengeksploitasi visibilitas pencarian dan kepercayaan pengguna.	Perluas kontrol ke ekosistem digital eksternal.
Le et al. (2025)	Aktivitas pengguna UKM	Pengembangan kerangka	Analitik perilaku pengguna dapat mendeteksi aktivitas abnormal.	Gunakan pemantauan perilaku secara layak dan etis.
Awan & Alam (2025)	Perusahaan kecil dan menengah	Pemetaan sistematis	Ancaman beragam, tetapi kapabilitas UKM belum matang.	Gunakan strategi keamanan siber yang terjangkau dan dapat diskalakan.
Khan et al. (2025b)	Dukungan siber bagi UKM	Studi empiris dukungan	UKM memerlukan panduan eksternal yang mudah diakses.	Bangun jejaring dengan penyedia keamanan siber dan akuntan.
Falch et al. (2023)	UKM Nordik-Baltik	Analisis strategi	Keamanan siber UKM harus praktis dan adaptif terhadap wilayah.	Selaraskan kontrol dengan ekosistem regional.
Aslan et al. (2023)	Sistem siber	Tinjauan komprehensif	Ancaman siber memerlukan respons teknis dan organisasi.	Rancang kerangka risiko kecurangan berlapis.

Tiwari (2025)	Usaha kecil	Analisis strategi terapan	Usaha kecil memerlukan perencanaan kesiapan yang dapat diskalakan.	Tanamkan pencegahan kecurangan dalam investasi keamanan siber.

Teknologi *Anti-Fraud*, *Data Analytics*, dan Deteksi *Fraud* Berbasis AI

Tabel 3 menyajikan sintesis berbagai penelitian mengenai pemanfaatan teknologi *anti-fraud* dalam mendukung deteksi dan pencegahan *fraud*. Bukti empiris yang paling kuat dikemukakan oleh Rugeles Diaz et al. (2025), yang menganalisis 221.292 data transaksi kartu dari *merchant payment gateway* di Amerika Latin. Hasil penelitian menunjukkan bahwa model analitik mampu mencegah sekitar 48–85% transaksi *fraud*, bergantung pada skala usaha (*merchant*) yang dianalisis. Temuan ini menunjukkan bahwa penerapan *data analytics* dapat meningkatkan efektivitas pencegahan *fraud* secara signifikan. Namun, tingkat keberhasilan model dipengaruhi oleh ukuran *merchant*, karakteristik pola transaksi, serta kebutuhan untuk melakukan pembaruan model secara berkelanjutan agar tetap mampu mendeteksi pola *fraud* yang terus berkembang.

Temuan tersebut didukung oleh penelitian Ridha Tarigan et al. (2025), yang menunjukkan bahwa teknologi *anti-fraud* memengaruhi perilaku *fraud* karyawan melalui peningkatan persepsi terhadap aktivitas pengawasan. Selain itu, Mohamad et al. (2026) mengemukakan bahwa penerapan *AI-powered mobile money* mampu meningkatkan kepercayaan pengguna sekaligus membantu UMKM mengurangi risiko *fraud* dalam transaksi rantai pasok (*supply chain*). Hasil-hasil tersebut menunjukkan bahwa efektivitas teknologi *anti-fraud* tidak hanya ditentukan oleh kemampuan sistem dalam mengidentifikasi transaksi yang mencurigakan, tetapi juga oleh kemampuannya dalam membentuk persepsi pengawasan dan meningkatkan kepercayaan para pengguna.

Berbagai penelitian teknis turut memperluas pemahaman mengenai model deteksi *fraud* yang dapat diterapkan pada sistem pembayaran digital. Ngai et al. (2011) mengklasifikasikan metode *data mining* berdasarkan jenis *fraud*, metode analisis, dan bidang penerapannya. Selanjutnya, Cherif et al. (2023), Carcillo et al. (2021), Alatawi (2025), Charizanos et al. (2024), Loukili et al. (2024), dan Chang et al. (2024) menunjukkan bahwa deteksi *credit-card fraud* maupun *e-payment fraud* semakin mengandalkan penerapan *machine learning*, model hibrida *supervised–unsupervised learning*, *fuzzy detection*, *deep learning*, serta analisis transaksi tingkat lanjut. Di sisi lain, Vijayanand et al. (2025) menekankan pentingnya penerapan *explainable artificial intelligence (XAI)* dalam deteksi *mobile money fraud* untuk meningkatkan transparansi proses pengambilan keputusan. Oleh karena itu, bagi UMKM, implementasi teknologi *anti-fraud* tidak hanya berfokus pada penggunaan teknologi yang canggih, tetapi juga pada pemilihan model yang mudah diinterpretasikan, terjangkau dari sisi biaya, sesuai dengan volume transaksi, kompatibel dengan data yang tersedia, serta didukung oleh mekanisme tata kelola (*governance*) yang akuntabel.

Tabel 3. Ringkasan Temuan Utama mengenai Teknologi *Anti-Fraud*, *Data Analytics*, dan Deteksi *Fraud* Berbasis AI

Referensi	Teknologi	Metode/Data	Temuan Utama	Implikasi
Rugeles Diaz et al. (2025)	Penambangan data, ML, RFM, MLP	221.292 rekaman kartu	Model mencegah 48%-85% transaksi curang, bergantung pada ukuran usaha.	Sesuaikan analitik dengan ukuran pedagang.
Ridha Tarigan et al. (2025)	TI anti-kecurangan	Analisis moderasi survei	Teknologi memoderasi pengaruh kesempatan dan rasionalisasi.	Gunakan pemantauan sebagai pencegah perilaku.
Mohamad et al. (2026)	Mobile money berbasis AI	Wawancara 40 pemilik UKM	Teknologi meningkatkan kepercayaan dan membantu mengatasi kecurangan.	Selaraskan perangkat pembayaran dengan kepercayaan dan regulasi.
Vijayanand et al. (2025)	Pembelajaran ansambel XAI	Deteksi kecurangan mobile money	AI yang dapat dijelaskan meningkatkan transparansi.	Gunakan peringatan yang dapat diinterpretasikan.
Ngai et al. (2011)	Klasifikasi penambangan data	Tinjauan literatur	Deteksi dapat dikelompokkan menurut jenis kecurangan, metode, dan ranah.	Gunakan pengodean analitik yang terstruktur.
Cherif et al. (2023)	Pembelajaran mesin dan mendalam	Tinjauan sistematis	Deteksi kecurangan kartu kredit semakin mengandalkan teknologi disruptif.	Gunakan model yang akurat dan terus diperbarui.
Carcillo et al. (2021)	Model hibrida terawasi/tak terawasi	Kecurangan kartu kredit	Pendekatan hibrida dapat mengatasi ketidakseimbangan data.	Cocok ketika data UKM berlabel terbatas.
Alatawi (2025)	Pembelajaran mesin berbasis IoT	Set data kartu kredit	Data IoT dapat mendukung deteksi kecurangan.	Amankan alur data UKM.
Charizanos et al. (2024)	Deteksi fuzzy daring	Transaksi kartu kredit	Model fuzzy mendukung peringatan daring yang adaptif.	Gunakan pemantauan waktu nyata yang fleksibel.
Loukili et al. (2024)	Pembelajaran mendalam	Kecurangan pembayaran elektronik	Pembelajaran mendalam meningkatkan keamanan pembayaran.	Padukan analitik dengan tata kelola.

Chang et al. (2024)	Pembelajaran mesin lanjut	Kecurangan pembayaran kartu	Pembelajaran mesin memperkuat investigasi kecurangan pembayaran.	Pilih model menurut transaksi dan ukuran usaha.
Dadhich et al. (2022)	Solusi kecurangan berbasis teknologi	Analisis tinjauan	Adopsi teknologi juga menciptakan jalur kecurangan baru.	Pantau risiko yang ditimbulkan digitalisasi.

Governance, Kepatuhan, Akuntansi Forensik, dan Ketahanan terhadap _Fraud_

Tabel 4 mengalihkan fokus pembahasan dari teknologi deteksi menuju aspek *governance* dan ketahanan organisasi (*fraud resilience*) dalam pengelolaan risiko *fraud*. Awolowo et al. (2026) berpendapat bahwa *cybersecurity assurance* pada UMKM tidak hanya ditentukan oleh penerapan teknologi, tetapi juga dipengaruhi oleh efektivitas *fraud risk management*, *forensic accounting*, serta budaya organisasi. Temuan tersebut sejalan dengan penelitian Moschella et al. (2023) yang menunjukkan bahwa akuntan memiliki peran penting dalam mendukung pengelolaan risiko UMKM melalui penerapan prosedur pengendalian, peningkatan disiplin pelaporan, dan dukungan terhadap proses pengambilan keputusan. Selain itu, Kumari Tiwari dan Debnath (2017) menjelaskan bahwa *forensic accounting* merupakan bidang multidisiplin yang mengintegrasikan akuntansi, audit, investigasi, hukum, dan analitik. Perspektif tersebut kemudian diperluas oleh Daraojimba et al. (2023), yang menegaskan bahwa lingkungan digital menuntut *forensic accounting* untuk mampu menangani bukti digital (*digital evidence*) serta berbagai bentuk manipulasi yang difasilitasi oleh perkembangan teknologi. Secara keseluruhan, berbagai penelitian tersebut menempatkan *forensic accounting* bukan hanya sebagai fungsi investigatif setelah terjadinya *fraud*, tetapi juga sebagai kapabilitas strategis yang mendukung pencegahan dan ketahanan organisasi.

Berbagai bukti empiris juga menunjukkan bahwa efektivitas *fraud risk management* berkaitan erat dengan kualitas *governance*, tingkat kepercayaan institusional, serta ketahanan keuangan organisasi. Zirar et al. (2026) menemukan bahwa penerapan *smart contracts* mampu meningkatkan transparansi, *traceability*, dan *trust* dalam transaksi UMKM. Namun, manfaat tersebut hanya dapat dicapai apabila diikuti dengan penyesuaian model bisnis dan penguatan sistem *governance*. Selanjutnya, Nato dan Bontempi (2022) menunjukkan bahwa efektivitas mekanisme pendanaan darurat bagi UMKM sangat bergantung pada keberadaan sistem pengendalian administratif yang kuat untuk mencegah penyalahgunaan dana. Di sisi lain, Narayan et al. (2025) mengaitkan kualitas *governance* dengan akses pembiayaan dan keberlanjutan (*sustainability*), dengan menunjukkan bahwa fragmentasi data *Environmental, Social, and Governance (ESG)* meningkatkan biaya pembiayaan UMKM sebesar 9–15%, sedangkan pemanfaatan *blockchain* dan analitik berbasis *artificial intelligence (AI)* mampu menurunkan risiko *green-bond fraud* hingga 18% di kawasan Asia Tenggara.

Penelitian Ferreira de Araújo Lima et al. (2020), Brustbauer (2016), dan Chakabva et al. (2021) secara konsisten menunjukkan bahwa penerapan manajemen risiko pada UMKM masih menghadapi berbagai kendala, seperti keterbatasan sumber daya, rendahnya tingkat formalisasi organisasi, serta minimnya keahlian dalam pengelolaan risiko. Kondisi tersebut

menunjukkan bahwa peningkatan ketahanan terhadap *fraud* tidak dapat dicapai hanya melalui adopsi teknologi, tetapi juga memerlukan sistem *governance* yang bersifat modular, terjangkau, serta disesuaikan dengan tingkat kematangan organisasi (*organizational maturity*). Oleh karena itu, pengelolaan risiko *fraud* pada UMKM perlu mengintegrasikan aspek tata kelola, pengendalian internal, *cybersecurity*, dan *forensic accounting* sebagai satu kesatuan yang saling mendukung dalam membangun ketahanan organisasi secara berkelanjutan.

Tabel 4. Ringkasan Temuan Utama mengenai *Governance*, Kepatuhan, Akuntansi Forensik, dan Ketahanan terhadap *Fraud*

Referensi	Fokus	Metode/Data	Temuan Utama	Implikasi
Awolowo et al. (2026)	Asurans keamanan siber	Kerangka konseptual	Budaya, manajemen risiko kecurangan, dan akuntansi forensik mendukung resiliensi UKM.	Jadikan resiliensi sebagai kapabilitas strategis.
Zirar et al. (2026)	Tata kelola kontrak pintar	Analisis resiliensi UKM	Kontrak pintar meningkatkan transparansi, keterlacakan, dan kepercayaan.	Selaraskan blockchain dengan kesiapan tata kelola.
Nato & Bontempi (2022)	Kontrol dana darurat	Analisis kasus Uni Eropa	Pencegahan bergantung pada pengendalian bertingkat yang kuat.	Seimbangkan kecepatan kebijakan dan pemeriksaan kepatuhan.
Narayan et al. (2025)	Tata kelola adaptif dan ESG	SLR dan kasus komparatif	Data ESG terfragmentasi menaikkan biaya pembiayaan 9%-15%; AI/blockchain menurunkan risiko obligasi hijau 18%.	Hubungkan pengelolaan kecurangan, kepercayaan pembiayaan, dan keberlanjutan.
Moschella et al. (2023)	Akuntan dalam manajemen risiko	Studi akuntansi UKM	Akuntan mendukung disiplin pelaporan dan keputusan.	Gunakan akuntan sebagai perantara risiko kecurangan.
Ferreira de Araújo Lima et al. (2020)	Manajemen risiko UKM	SLR dan bibliometrik	Literatur manajemen risiko UKM masih terfragmentasi.	Integrasikan risiko kecurangan, siber, dan operasional.
Brustbauer (2016)	Manajemen risiko	Model struktural	UKM memerlukan ERM yang sesuai dengan	Kembangkan model kematangan yang

	perusahaan		ukuran dan sumber daya.	disesuaikan.
Chakabva et al. (2021)	Hambatan manajemen risiko	UKM pasar berkembang	Keterbatasan sumber daya, keahlian, dan sistem formal menghambat manajemen risiko.	Gunakan kontrol yang terjangkau dan dapat diskalakan.
Kumari Tiwari & Debnath (2017)	Akuntansi forensik	Sintesis pengetahuan	Akuntansi forensik memadukan akuntansi, audit, investigasi, hukum, dan analitik.	Bangun kapabilitas forensik pada UKM.
Daraojimba et al. (2023)	Akuntansi forensik digital	Analisis kecurangan digital	Kecurangan digital memerlukan bukti dan metode sadar siber.	Perluas investigasi menuju asurans digital.
Bozkus Kahyaoglu & Caliyurt (2018)	Audit internal dan asurans siber	Perspektif audit	Audit internal perlu mencakup risiko siber dan tata kelola teknologi.	Jembatani audit, keamanan siber, dan asurans kecurangan.
Chih-Hao & Kuen-Chang (2020)	Peta strategi risiko kecurangan	Model keputusan	Manajemen risiko kecurangan dapat diintegrasikan melalui sasaran dan indikator.	Gunakan tata kelola terstruktur untuk pencegahan dan respons.

PEMBAHASAN

Hasil sintesis menunjukkan bahwa risiko *fraud* pada UMKM yang sedang mengalami transformasi digital memiliki karakteristik yang multidimensional. Risiko tersebut tidak dapat dijelaskan hanya dari satu aspek, seperti perilaku karyawan, *cybercrime*, manipulasi akuntansi, maupun *payment fraud*. Sebaliknya, *fraud* muncul sebagai konsekuensi dari interaksi antara perilaku individu, kelemahan *internal control*, kerentanan teknologi, sistem transaksi digital, mekanisme kepercayaan pada platform digital, serta keterbatasan sumber daya organisasi. Temuan ini mengintegrasikan bukti empiris mengenai *internal fraud* yang dikemukakan oleh Andoh et al. (2018), faktor perilaku yang dijelaskan oleh Ridha Tarigan et al. (2025), ancaman *cybersecurity* yang diidentifikasi oleh Loskorikh et al. (2025), serta risiko pada platform digital yang dibahas oleh Oo et al. (2025). Dari perspektif teoretis, hasil kajian ini memperluas penerapan *Fraud Triangle Theory* dan *Fraud Diamond Theory* dengan menunjukkan bahwa transformasi digital tidak hanya memperbesar peluang (*opportunity*) dan kapabilitas (*capability*) dalam melakukan *fraud*, tetapi juga menciptakan bentuk-bentuk baru rasionalisasi (*rationalization*) serta persepsi legitimasi terhadap tindakan tersebut.

Cybersecurity dan *internal control* seharusnya dipandang sebagai dua komponen yang saling melengkapi, bukan sebagai fungsi yang berdiri sendiri. *Cybersecurity* berperan dalam melindungi infrastruktur teknologi, sedangkan *internal control* memastikan bahwa setiap transaksi telah memperoleh otorisasi yang memadai, ditinjau secara tepat, didokumentasikan

dengan baik, dan dapat dipertanggungjawabkan. Perkembangan sistem akuntansi digital, aplikasi berbasis web, dan platform pembayaran digital semakin mengaburkan batas antara kedua fungsi tersebut. Sebagai contoh, *invoice fraud* dapat terjadi akibat kombinasi beberapa kelemahan sekaligus, seperti akun *email* yang telah dikompromikan, mekanisme autentikasi yang lemah, proses verifikasi pemasok yang kurang memadai, serta lemahnya proses peninjauan akuntansi. Bukti empiris yang menunjukkan bahwa penerapan *multi-factor authentication*, pelatihan karyawan, serta kolaborasi antara fungsi teknologi informasi dan akuntansi mampu menurunkan risiko siber sekaligus mempercepat penyelesaian insiden (Loskorikh et al., 2025) mendukung konsep pengendalian *socio-technical* berlapis (*layered socio-technical control model*). Model tersebut juga menjelaskan mengapa akuntan tetap memiliki peran sentral dalam pengelolaan risiko pada UMKM (Moschella et al., 2023).

Pemanfaatan teknologi *anti-fraud* menawarkan potensi yang besar dalam mendukung pencegahan dan deteksi *fraud*, namun teknologi tersebut tidak dapat diposisikan sebagai solusi yang bersifat universal. Penelitian Rugeles Diaz et al. (2025) menunjukkan bahwa *machine learning* dan *data analytics* mampu mencegah sebagian besar transaksi *fraud*. Meskipun demikian, efektivitas model tersebut sangat bergantung pada ketersediaan data yang memadai, proses pembaruan model secara berkala, serta kemampuan dalam menginterpretasikan hasil analisis. Penelitian Mohamad et al. (2026) juga menunjukkan bahwa penerapan *AI-powered mobile money* mampu meningkatkan kepercayaan pengguna sekaligus mengurangi risiko *fraud* pada rantai pasok UMKM. Namun, efektivitas teknologi tersebut dipengaruhi oleh regulasi, kompleksitas implementasi, tingkat kemudahan penggunaan, serta kondisi geopolitik. Di sisi lain, Zirar et al. (2026) menjelaskan bahwa *smart contracts* mampu meningkatkan kepercayaan (*trust*) dan keterlacakan (*traceability*) transaksi, tetapi implementasinya memerlukan penyesuaian model bisnis dan tata kelola organisasi. Oleh karena itu, hasil kajian ini menegaskan bahwa penerapan teknologi *anti-fraud* harus didukung oleh *governance*, budaya etika, program pelatihan, serta mekanisme pengambilan keputusan yang akuntabel sehingga manfaat teknologi dapat dioptimalkan secara berkelanjutan.

Kajian ini juga mengidentifikasi sejumlah keterbatasan metodologis dalam penelitian mengenai *fraud risk management*. Berbagai penelitian yang dianalisis menunjukkan perbedaan yang cukup besar dalam hal metode penelitian, konteks organisasi, jenis *fraud*, maupun tingkat analisis yang digunakan. Sebagian penelitian secara langsung berfokus pada UMKM, seperti Andoh et al. (2018), Ridha Tarigan et al. (2025), Mohamad et al. (2026), dan Rugeles Diaz et al. (2025). Sementara itu, penelitian lainnya memberikan bukti yang berasal dari konteks akuntansi, *cybersecurity*, *credit-card fraud*, maupun *governance*, yang kemudian dapat diadaptasi untuk konteks UMKM. Tingginya tingkat heterogenitas tersebut menyebabkan pendekatan *meta-analysis* kurang sesuai digunakan sehingga penelitian ini memilih pendekatan *thematic synthesis*. Selain itu, masih terbatas penelitian longitudinal yang mampu menjelaskan bagaimana UMKM mengimplementasikan, memelihara, dan memperbarui sistem pengendalian *fraud* dari waktu ke waktu. Bukti komparatif antar sektor industri, ukuran perusahaan, maupun wilayah geografis juga masih relatif terbatas. Demikian pula, masih sedikit penelitian yang membahas bagaimana UMKM menyeimbangkan aspek privasi, pengawasan, kepercayaan karyawan, dan penerapan analitik *fraud* dalam aktivitas operasionalnya.

Berdasarkan keseluruhan temuan tersebut, penelitian ini menawarkan suatu kerangka *socio-technical* dalam pengelolaan risiko *fraud* pada UMKM berbasis digital. Pada tingkat perilaku (*behavioral level*), UMKM perlu mengelola faktor tekanan (*pressure*), peluang

(*opportunity*), rasionalisasi (*rationalization*), dan kapabilitas (*capability*). Pada tingkat proses (*process level*), organisasi memerlukan *internal control*, prosedur akuntansi, mekanisme verifikasi, serta akuntabilitas yang memadai. Selanjutnya, pada tingkat teknologi (*technical level*), diperlukan penerapan *cybersecurity controls*, aplikasi yang aman, *data analytics*, serta sistem deteksi *fraud*. Sementara itu, pada tingkat tata kelola (*governance level*), organisasi memerlukan kapabilitas *forensic accounting*, kepatuhan terhadap regulasi, dukungan dari pihak eksternal, serta kemampuan belajar dan beradaptasi secara berkelanjutan. Kerangka tersebut menghubungkan *fraud risk management* dengan perspektif *resource-based view* dan *dynamic capabilities*, yang menekankan bahwa ketahanan terhadap *fraud* dibangun melalui pengembangan sumber daya yang bernilai, sulit ditiru, serta tertanam dalam organisasi, seperti budaya yang sadar terhadap keamanan siber, sistem pengendalian yang didukung oleh akuntan, kompetensi *forensic accounting*, pemantauan berbasis data, serta *adaptive governance*. Penelitian selanjutnya disarankan untuk menguji kerangka ini secara empiris pada berbagai sektor UMKM, mengembangkan model kematangan (*fraud-risk maturity model*), mengevaluasi penerapan teknologi *anti-fraud* berbasis *explainable artificial intelligence (XAI)* yang terjangkau, serta mengkaji ekosistem pembayaran digital di negara berkembang.

KESIMPULAN, KETERBATASAN, DAN SARAN

Kesimpulan

Penelitian ini menggunakan pendekatan systematic literature review untuk mengkaji fraud risk management pada UMKM yang sedang mengalami transformasi digital melalui sintesis berbagai bukti mengenai internal fraud, ancaman cybersecurity, risiko akuntansi digital, teknologi anti-fraud, governance, forensic accounting, dan ketahanan organisasi. Hasil kajian menjawab pertanyaan penelitian dengan menunjukkan bahwa UMKM digital menghadapi berbagai bentuk risiko fraud yang saling berkaitan. Internal fraud konvensional masih menjadi tantangan utama, sementara transformasi digital memperluas paparan terhadap cyber fraud, payment fraud, penipuan pada platform digital, kerentanan aplikasi web, serta manipulasi berbasis data. Cybersecurity, internal control, dan forensic accounting memberikan kontribusi yang paling efektif apabila diterapkan secara terpadu sebagai pengendalian socio-technical yang berlapis, bukan sebagai fungsi yang terpisah. Selain itu, berbagai teknologi anti-fraud, seperti artificial intelligence (AI), machine learning, user-behavior analytics, multi-factor authentication, blockchain, dan smart contracts, mampu meningkatkan efektivitas pencegahan maupun deteksi fraud. Namun demikian, keberhasilan implementasinya sangat dipengaruhi oleh keterjangkauan biaya, tingkat explainability, kesiapan governance, budaya etika organisasi, serta kemampuan organisasi untuk terus belajar dan beradaptasi. Kontribusi utama penelitian ini terletak pada penempatan fraud risk management sebagai suatu kapabilitas adaptif (adaptive capability) dalam UMKM digital. Kapabilitas tersebut mengintegrasikan Fraud Theory, resourcebased view, dynamic capabilities, cybersecurity assurance, internal control, dan forensic accounting ke dalam satu kerangka konseptual yang komprehensif. Selain itu, penelitian ini juga mengidentifikasi beberapa kesenjangan penelitian yang masih memerlukan perhatian, antara lain terbatasnya bukti longitudinal, masih minimnya validasi teknologi anti-fraud berbasis AI yang secara khusus ditujukan bagi UMKM, belum optimalnya integrasi antara penelitian cybersecurity dan akuntansi, serta terbatasnya bukti empiris dari negara berkembang yang memiliki keterbatasan sumber daya. Oleh karena itu, penelitian selanjutnya diharapkan dapat mengembangkan model kematangan fraud risk management yang lebih skalabel, menguji

penerapan analitik antifraud berbasis explainable artificial intelligence (XAI) yang sesuai dengan karakteristik UMKM, serta mengeksplorasi bagaimana akuntan, penyedia layanan cybersecurity, platform digital, dan regulator dapat berkolaborasi dalam memperkuat ketahanan UMKM terhadap risiko fraud.

Keterbatasan

Kajian ini dibatasi oleh heterogenitas metode, konteks, jenis kecurangan, dan tingkat analisis pada studi yang ditelaah. Sebagian bukti berasal dari konteks akuntansi, keamanan siber, pembayaran kartu, dan tata kelola yang tidak seluruhnya berfokus langsung pada UMKM. Selain itu, bukti longitudinal, perbandingan lintas sektor dan wilayah, serta kajian mengenai keseimbangan antara privasi, pengawasan, dan kepercayaan karyawan masih terbatas. Keterbatasan tersebut membatasi generalisasi temuan dan menyebabkan sintesis tematik lebih sesuai daripada meta-analisis.

Saran

Penelitian selanjutnya perlu menguji kerangka sosio-teknis ini secara empiris pada berbagai sektor dan skala UMKM, mengembangkan model kematangan risiko kecurangan yang terjangkau, serta mengevaluasi analitik antikecurangan berbasis explainable artificial intelligence. Kajian mendatang juga perlu menilai bentuk kolaborasi yang efektif antara akuntan, penyedia layanan keamanan siber, platform digital, dan regulator dalam memperkuat ketahanan UMKM terhadap kecurangan.

DAFTAR PUSTAKA

Albrecht, W. S., Albrecht, C. C., Albrecht, C. O., & Zimbelman, M. F. (2019). *Fraud Examination (6th ed.)*. Cengage Learning.

Andoh, C., Quaye, D., & Akomea-Frimpong, I. (2018). Impact of fraud on Ghanaian SMEs and coping mechanisms. *Journal of Financial Crime*, *25*(2), 400–418.

Aslan, O., Aktug, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333.

Awolowo, I. F., Ode, E., Abidoye, A., Ajao, O., & Jogunola, O. (2026).

Cybersecurity assurance for SMEs: A conceptual framework integrating organizational culture, fraud risk management and forensic accounting. *Canadian Journal of Administrative Sciences/Revue Canadienne des Sciences de l'Administration*, *43*(1), e70051.

Barney, J. B. (1991). Firm resources and sustained competitive advantage.

Journal of Management, *17*(1), 99–120.

Bozkus Kahyaoglu, S., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal*, *33*(4), 360–376.

Brustbauer, J. (2016). Enterprise risk management in SMEs: Towards a structural model. *International Small Business Journal*, *34*(1), 70–85.

Carcillo, F., Le Borgne, Y.-A., Caelen, O., Kessaci, Y., Oble, F., & Bontempi, G. (2021). Combining unsupervised and supervised learning in credit card fraud detection. *Information Sciences*, *557*, 317–331.

Chakabva, O., Tengeh, R., & Dubihlela, J. (2021). Factors inhibiting effective risk management in emerging market SMEs. Journal of Risk and Financial Management, 14(6).

Chang, V., Ali, B., Golightly, L., Ganatra, M. A., & Mohamed, M. (2024).

Investigating credit card payment fraud with detection methods using advanced machine learning. *Information*, *15*(8), 478.

Cressey, D. R. (1950). The criminal violation of financial trust. *American Sociological Review*, *15*(6), 738–743.

Daraojimba, R. E., Farayola, O. A., Olatoye, F. O., Mhlongo, N., & Oke, T. T. (2023). Forensic accounting in the digital age: A US perspective. *Finance & Accounting Research Journal*, *5*(11), 342–360.

Eisenhardt, K. M., & Martin, J. (2000). Dynamic capabilities: What are they?

Strategic Management Journal, 21(10–11), 1105–1121.

Ferreira de Araújo Lima, P., Crema, M., & Verbano, C. (2020). Risk management in SMEs: A systematic literature review and future directions. *European Management Journal*, *38*(1), 78–94.

Jans, M., Lybaert, N., & Vanhoof, K. (2009). A framework for internal fraud risk reduction at IT integrating business processes: The IFR2 framework. *The International Journal of Digital Accounting Research*, *9*, 1–29.

Khan, N., Furnell, S., Bada, M., Rand, M., & Nurse, J. R. C. (2025). Investigating the experiences of providing cyber security support to small- and medium-sized enterprises. *Computers & Security*, *154*, 104448.

Khan, S. A., Azim, N., Iqbal, A., Abbas, H., & Qureshi, S. (2025). Securing web applications: A practical approach to mitigating OWASP Top 10 vulnerabilities. *VFAST Transactions on Software Engineering*, *13*(2), 273–291.

Kumari Tiwari, R., & Debnath, J. (2017). Forensic accounting: A blend of knowledge. *Journal of Financial Regulation and Compliance*, *25*(1), 73–85.

Le, T. D., Le Dinh, T., & Uwizeyemungu, S. (2025). A cybersecurity framework for enhancing small and medium-sized enterprises security posture using user behaviour analytics. *Enterprise Information Systems*, *19*(10), 2529282.

Le, T. D., Le-Dinh, T., & Uwizeyemungu, S. (2024). Search engine optimisation poisoning: A cybersecurity threat analysis and mitigation strategies for small and medium-sized enterprises. *Technology in Society*, *76*, 102470.

Loskorikh, G., Shebeshten, E., Koval, O., Bagrii, K., & Valkova, N. (2025). Risks of cyberattacks on accounting: Analysis of modern threats and preventive measures. *Sustainable Engineering and Innovation*, *7*(2), 493–506.

Low, P. (2017). Insuring against cyber-attacks. *Computer Fraud & Security*, *2017*(4), 18-20.

Mohamad, M., Laryeafio, M. N., Koroye, E., Nyame, D., Ayertey, S., & Emini, A. (2026). The impact of AI-powered mobile money system on supply chain: Multi-cases from SMEs in the Global South. *International Journal of Interactive Mobile Technologies*, *20*(1), 105–121.

Moschella, J., Boulianne, E., & Magnan, M. (2023). Risk management in small-and medium-sized businesses and how accountants contribute.

Contemporary Accounting Research, *40*(1), 668–703.

Narayan, M., Kumar, N., Parida, V. K., & Kumari, P. (2025). Sustainable finance in emerging markets: Adaptive governance and environmental, social, and governance innovation for equitable climate resilience.

Development and Sustainability in Economics and Finance, *8*, 100101.

Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems*, *50*, 559–569.

Oo, P. P., Thomas, H., Allison, & Hmieleski, K. M. (2025). The dark side of source credibility: Differential effectiveness of credibility cues in fraudulent versus legitimate crowdfunding campaigns. Journal of Business Ethics.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow,

C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder,

E. W., Mayo-Wilson, E., McDonald, S., ... Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, *372*, n71.

Ridha Tarigan, N. M., Simbolon, R., & Elviani, S. (2025). Reducing unethical behavior in SMEs using fraud triangle theory and anti-fraud technology: A case study from Medan City. *Heritage and Sustainable Development*, *7*(2), 1341–1350.

Rugeles Diaz, L. T., Echarte Fernández, M. Á., Jorge-Vázquez, J., & Nañez Alonso,

S. L. (2025). Data analytics to prevent retail credit card fraud: Empirical evidence from Latin America. *Financial Innovation*, *11*(1), 137.

Suh, J. B., Nicolaides, R., & Trafford, R. (2019). The effects of reducing opportunity and fraud risk factors on the occurrence of occupational fraud in financial institutions. *International Journal of Law, Crime and Justice*, *56*, 79–88.

Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of sustainable enterprise performance. *Strategic Management Journal*, *28*(13), 1319–1350.

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, *18*(7), 509–533.

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British Journal of Management*, *14*(3), 207–222.

Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research*, *122*, 889–901.

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *Journal of Strategic Information Systems*, *28*(2), 118–144.

Vijayanand, D., Smrithy, G. S., & Vaardhini, M. S. (2025). Explainable AI-enhanced ensemble learning for financial fraud detection in mobile money transactions. *Intelligent Decision Technologies*, *19*(1), 52-67.

Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *CPA Journal*, *74*(12), 38–42.

Xiao, Y., & Watson, M. (2019). Guidance on conducting a systematic literature review. *Journal of Planning Education and Research*, *39*(1), 93–112.

Zirar, A., Jabbar, A., & Mahdiraji, H. A. (2026). Smart contracts and SME resilience: Business model adaptation and international considerations. *Canadian Journal of Administrative Sciences*, *43*(1), e70046.